Formosa Journal of Science and Technology (FJST)
Vol. 4, No. 9, 2025: 3015-3030

Judicial Adaptation to Digital Evidence in the Era of Cyber Governance

Yanto Irianto
Universitas Nahdlatul Ulama Cirebon, Indonesia
Corresponding Author: Yanto Irianto, yantoirianto755@gmail.com

A R T I C L E I N F O

Keywords: Judicial Adaptation, Digital Evidence, Cyber Governance.

Received : 11, August
Revised : 25, August
Accepted : 28, September

A B S T R A C T

This study examines how the Indonesian judiciary adapts to the use of digital evidence within the framework of cyber governance. Using an empirical juridical approach that combines normative legal analysis with empirical data from interviews with 12 legal practitioners and case studies at the Cirebon District Court, the research reveals that while legal provisions formally recognize digital evidence, challenges remain in technical verification, institutional capacity, and judicial interpretation. The findings indicate that judicial adaptation is still in transition, requiring stronger procedural guidelines, enhanced law enforcement capacity, and integration of forensic expertise. This study contributes to the legal discourse on digital evidence and offers practical recommendations to improve the judiciary's effectiveness in handling cyber-related cases.

ISSN-E: 2964-6804
DOI: https://doi.org/10.55927/fjst.v4i9.248
https://traformosapublisher.org/index.php/fjst

INTRODUCTION

The development of information and communication technology over the past decade has changed the way evidence is collected, stored, and presented in judicial proceedings. Electronic data including server logs, metadata, instant messages, multimedia recordings, and IoT device outputs are now a key component in many criminal and civil cases, thus demanding procedural and technical adaptation from judicial institutions (National Institute of Justice, 2020). This transformation is not only about the adoption of software or electronic file filling systems, but also touches on the aspects of evidentiary legitimacy, authentication, and chain of custody that determine the evidentiary value of court decisions (Pew Charitable Trusts, 2021).

Globally, a review of the digital forensic literature and cross-country review show a consensus, among others, that courts are under double pressure to recognize and assess electronic evidence legally and fairly, that courts are facing limited technical capacity and inadequate procedural frameworks (Reedy, 2023). Empirical studies on law enforcement actors highlight the need for specialized training, uniform electronic evidence management protocols, and close working relationships between investigators, digital forensics, and prosecutors in order for digital evidence to be used effectively at trial (Miller et al., 2022). On the other hand, technological developments such as end-to-end encryption and media manipulation add to the complexity of electronic proof verification (Stoykova, 2024).

In the Indonesian context, the regulation regarding electronic evidence has been accommodated in Law (UU) Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, especially Article 5 paragraph (1) of the ITE Law which emphasizes that electronic information and/or electronic documents and their printed results can be used as evidence. The Constitutional Court in Decision No. 20/PUU-XIV/2016 affirmed the restriction on the use of electronic evidence obtained through means that violate the provisions of the law (Constitutional Court Decision No. 20/PUU-XIV/2016). In addition, the administration of electronic cases is further regulated by Supreme Court Regulations, including amendments to PERMA related to e-court and e-litigation (Supreme Court Regulation Number 7 of 2022), which provide an administrative framework but have not resolved issues of technical verification and forensic capacity at the regional level (Supreme Court, 2022).

Despite the normative foundation, previous studies in Indonesia tend to focus on formal legal and technical aspects of forensics separately. For example, juridical studies examine the legal force of electronic evidence (Yulianto, 2020), while technical studies highlight the method of collecting and preserving digital evidence (Ashari, 2020). However, few studies have integrated normative analysis with empirical field data on how judges, prosecutors, and advocates in local courts actually assess, receive, or reject digital evidence a methodological gap that hinders applicable policy recommendations (Santoso, 2024). This gap underscores the need for a socio-legal study that combines regulatory review with interviews and case studies at the provincial/district court level.

Recent international studies confirm the relevance of such approaches: cross-border studies and Interpol reviews suggest the integration of technical standards with clear procedural guidelines as well as the improvement of forensic human resources to maintain the integrity of the judicial process (Reedy, 2023). In addition, research surveying public prosecutors and investigators found that specialization in digital evidence handling, inter-institutional cooperation, and electronic evidence management policies significantly increased the utilization of digital evidence in the prosecution process (Miller et al., 2022). In the realm of legal theory, the governance-oriented approach requires an examination of how cyber governance, namely data governance, cybersecurity, and technology regulation, interact with traditional evidentiary principles in respecting the guarantee of fair process (Stoykova, 2024).

Based on the identification of the gap, this study was formulated with the objectives: (1) to analyze the extent to which the national legal framework, especially the provisions of the ITE Law and Supreme Court regulations, accommodate the principles of authentication and the legality of electronic evidence; (2) describe the adaptation practices of judicial actors (judges, prosecutors, advocates) in the District Court at the regional level, especially in Cirebon, to the challenge of technical verification of digital evidence; and (3) formulate policy recommendations that integrate procedural guidelines, digital forensic capacity building, and governance mechanisms to strengthen the credibility of electronic evidence. The goal is positioned to close the gap between written norms and empirical court practice, so that the resulting recommendations can be operational and implementable.

The contribution of this research is twofold. Theoretically, the research seeks to develop the legal discourse of proof by incorporating the perspective of cyber governance connecting traditional theory of proof, data governance, and digital forensic security as new analytical frameworks that are relevant in the digital era. In practice, the findings are expected to produce practical procedural guidelines, the need for integrated training for judicial officials, and a model of integration of forensic personnel in the trial process that can be adapted by local courts in Indonesia. Thus, this study is expected to enrich the international literature as well as provide policy input that is applicable to judicial reform at the local level.

THEORETICAL REVIEW

Transformation of the Digital Evidence Paradigm in the Judicial System

The development of information technology has changed the way people interact, transact, and leave a trail of activity. Every digital activity, from conversations on social media to online financial transactions, has the potential to become relevant evidence in court. This marks a paradigm shift from traditional evidence, such as physical documents and direct witnesses, to digital evidence that is invisible and often cross-jurisdictional. According to research, the biggest challenge of digital evidence is how to ensure that it remains authentic, verifiable, and has the same legal value as conventional evidence (Kenneally & Brown, 2022). This transformation requires serious adaptation in

judicial procedures so that the legal system remains able to respond to the dynamics of the digital society.

Authentication, Integrity, and Chain of Custody

The acceptance of digital evidence in court is highly determined by its ability to be proven authentic and its integrity maintained since it was first collected. This process is known as a chain of custody, which is detailed documentation of who handles the evidence, when, where, and for what purpose. If this chain is broken or not well documented, the evidence may be considered invalid by the judge. Recent studies emphasize the importance of implementing technical standards such as hash verification and encryption to strengthen the validity of evidence (Karagiannis et al., 2021). Therefore, in addition to technological devices, the role of disciplined law enforcement in documentation procedures is key so that digital evidence can be legally accepted in court.

Technical Challenges and the Role of Digital Forensic Experts

Digital evidence is often stored in complex systems, such as cloud computing, Internet of Things devices, and encrypted data. This complexity presents a great challenge for investigators and judges in understanding the validity of evidence. The role of digital forensic experts is essential for bridging the gap between technical analysis and legal language. Research confirms that the quality of digital evidence submitted to the court depends on the ability of experts to explain the forensic process simply but still accurately (Ahmed & Khan, 2023). Thus, the judiciary's adaptation to digital evidence is not only institutional, but also requires the support of qualified technical expertise.

Standardization of Procedures and Harmonization of Regulations

The inconsistency of procedures in the management of digital evidence in various countries has become a serious problem in the era of legal globalization. Some jurisdictions have adopted international standards, such as ISO/IEC 27037, which provide guidance on how to legally identify, collect, and store digital evidence. The application of this standard has been proven to improve the consistency of judicial practice and strengthen the position of digital evidence in trials (Feki & Slimi, 2020). However, challenges still arise when cases involve more than one jurisdiction, as differences in national law can affect the validity of evidence. Therefore, the harmonization of international regulations is important so that digital evidence does not lose its legal force just because of differences in procedures between countries.

Cyber Governance, Human Rights and Legal Implications

The era of cyber governance puts digital evidence in a unique position: on the one hand it becomes an important instrument for enforcing the law, but on the other hand it has the potential to give rise to human rights violations, particularly the right to privacy. Data protection policies often clash with the authority of the authorities to access information. According to recent research, courts in various jurisdictions are still looking for a balance point between the

protection of individual privacy and the public interest in law enforcement (Schuppli, 2021). This shows that judicial adaptation to digital evidence cannot be separated from the broader cyber governance framework, so legal reform must pay attention to aspects of ethics, transparency, and accountability.

METHODOLOGY

Research Type and Design

This study uses an empirical juridical method that combines normative analysis and empirical studies. The normative analysis is focused on legal rules, such as the ITE Law, the Criminal Code, and PERMA e-Court/e-Litigation, as well as court decisions related to digital evidence. This analysis aims to understand the legal foundations and principles that govern the use of digital evidence. Meanwhile, empirical studies were conducted to explore judicial practices in the field, including how judges, prosecutors, advocates, and digital forensic experts assess and use digital evidence in trials (Klasén, 2024; Qureshi, 2024). This combination approach allows research to identify gaps between formal legal theory and real practice in court.

Research Location

The research was carried out at the Cirebon District Court as the main locus, where field research can be carried out through observation and case studies involving digital evidence. Additional locations include the Cirebon District Attorney's Office and the Cirebon Police, in order to get the perspective of law enforcement officials related to the investigation and prosecution process. Additional resource persons consisted of advocates and digital forensics experts in West Java, to complement data on technical practices and professional experience in assessing digital evidence.

Data Source

This study uses two main data sources. Primary data was obtained through in-depth interviews with judges, prosecutors, advocates, and digital forensic experts, as well as observation and case studies with digital evidence at the Cirebon District Court. Secondary data are derived from laws and regulations, legal doctrines, court rulings, legal literature, and journal articles relevant to the topic of digital evidence and cyber governance (Ahmed & Khan, 2023; Ratul et al., 2024). The combination of these data sources ensures that normative and empirical analysis can be carried out comprehensively.

Data Collection Techniques

Data collection is carried out through several techniques. First, literature studies to examine regulations, doctrines, and court decisions as a normative basis. Second, semi-structured interviews with purposively selected sources, which allowed researchers to explore experiences, perceptions, and practices of using digital evidence. Third, a case study in the form of direct observation of the trial process at the Cirebon District Court, to understand how digital evidence is used, analyzed, and tested in court (Quick & Choo, 2022).

Data Analysis Techniques

The data was analyzed using qualitative methods. Normative analysis is carried out through grammatical, systematic, and teleological legal interpretations of laws, PERMA, and court decisions. Empirical analysis is carried out using a thematic analysis approach, starting from the coding process, categorization, to interpretation. The results of normative and empirical analysis are then synthesized to assess the extent to which the judiciary has adapted to digital evidence and to identify technical and legal obstacles in the field (Klasén, 2024; Bérubé, 2025).

RESULTS AND DISCUSSION

Normative Foundations and Digital Evidence Recognition

The results of the normative analysis show that the Indonesian legal system has provided a strong formal basis for the recognition of digital evidence as a valid evidence in the judicial process. This recognition is explicitly regulated in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law). Article 5 paragraph (1) of the Law states that electronic information and/or electronic documents and their printed results can be used as valid legal evidence. This provision marks a paradigm shift from traditional evidentiary law that originally only recognized physical evidence such as paper documents, witnesses, or letters, to the recognition of digital evidence born from electronic activities.

In addition, normative strengthening can also be seen from the Constitutional Court Decision Number 20/PUU-XIV/2016, which affirms the principle of legality in the use of digital evidence. The ruling emphasizes that electronic evidence obtained through unlawful means, such as the results of illegal hacking or unauthorized wiretapping, is not admissible in court. Thus, even if the state recognizes the existence of digital evidence, its use must still be within the procedural law corridor that upholds human rights and the principle of fair trial.

In the administrative realm, Supreme Court Regulation (PERMA) Number 7 of 2022 concerning Electronic Case Administration and Trials provides a technical framework for the implementation of electronic trials (e-court and e-litigation). This regulation allows the submission of lawsuits, answers, replicas, duplicates, and proof electronically. However, the PERMA focuses more on case administration and has not comprehensively regulated a technical verification mechanism for the authenticity of digital evidence, such as metadata authentication, hash code validation, or chain of custody documentation standards.

Research findings in the field show that there is a gap between legal norms and empirical practice. On the one hand, judges and prosecutors at the Cirebon District Court recognize the legality of digital evidence as part of the evidentiary system. However, on the other hand, there are doubts and differences in interpretation when it comes to assessing the technical validity of the evidence. For example, electronic documents in the form of screenshots are often submitted as evidence, but their authenticity cannot necessarily be ascertained without the

support of digital forensic analysis. This has the potential to cause differences in verdicts between judges due to the absence of uniform procedural guidelines.

This condition shows that the established normative foundation is still in the transition phase to effective operationalization. Without clear technical standards, legal recognition of digital evidence risks being only a formality without being able to answer the need for valid proof in the digital age. In other words, a normative framework is in place, but implementing instruments such as authentication technical guidelines, digital forensic guidance, and capacity building of law enforcement are still not integrated.

From the perspective of cyber governance, the weak integration between norms and practices shows that digital judicial governance in Indonesia is still partial. Cyber governance requires synergy between legal regulations, technological infrastructure, and human resource capacity. Without a balance of these three aspects, the judicial process is not only prone to inconsistencies, but can also raise questions about the legitimacy of decisions. Thus, strategic steps are needed in the form of the preparation of technical standards for digital evidence authentication, training for law enforcement officials, and the establishment of a special digital forensic unit in local courts to strengthen the credibility of digital evidence before the law.

Adaptation Practices of Judges, Prosecutors, and Advocates in the Cirebon District Court

The results of empirical research through interviews with 12 informants consisting of judges, prosecutors, advocates, and digital forensic experts show that the practice of judicial adaptation to digital evidence in the Cirebon District Court is still at the **Transition phase**. Although normatively digital evidence has been recognized as legitimate according to Law Number 1 of 2024 concerning ITE, its implementation in the courtroom faces various complex dynamics.

Judge's Perspective

Most of the judges interviewed stated that digital evidence is now an inevitable part of the process of proving cases, both criminal and civil. Judges tend to accept submitted digital evidence, especially if it is supported by other evidence such as witnesses or physical documents. However, the study found that there is a **Differences in interpretation regarding the power of proof**. Some judges consider that digital evidence from social media or instant messaging applications can only be used as a **Proof of Clues**, is not the main evidence, as it is prone to manipulation and difficult to verify without the support of forensic analysis. A judge confirmed, "*If digital evidence is like a WhatsApp screenshot, it is indeed acceptable, but usually only as a clue. Without the support of witnesses or other evidence, we find it difficult to make it the main basis for the verdict.*" (Interview, H1, June 18, 2025). Other judges also highlighted authentication issues: "*Judges must be careful, because digital evidence is easy to manipulate. We often don't have the tools or experts to ensure its authenticity at trial.*" (Interview, H2, June 18, 2025).

Prosecutor's Perspective

The prosecutor showed a relatively more pragmatic attitude. They emphasize that digital evidence rarely stands alone, but rather must be linked to **Other evidence** according to the Criminal Code, such as witness statements or letters. In practice, prosecutors try to present digital evidence as a **Amplifier** from the series of evidence, not as the sole basis for prosecution. A prosecutor said, "*We usually don't use digital evidence as a single piece of evidence, but as a corroboration. If there is an electronic conversation, it must still be matched with witness statements or physical documents.*" (Interview, J1, June 19, 2025). However, the prosecutor also acknowledged technical limitations: "*For the validation of digital evidence, we rely heavily on the results of forensic laboratories. If there are no results, the trial process can be hampered.*" (Interview, J2, June 19, 2025).

Advocate's Perspective

From the advocate's side, the dominant approach is **Skeptical and critical** against the digital evidence submitted by the prosecutor and the opposing party. Advocates often question **chain of custody** Digital evidence, namely whether the evidence has been maintained authenticity since it was first collected until submitted at trial. An advocate asserted, "*We always ask, who first accesses the data? Is there an official record of who kept it? If the chain of custody is not clear, we can refute the evidence.*" (Interview, A1, June 19, 2025). Another advocate added, "*Digital evidence is vulnerable to engineering. If it's just a screenshot, it's very easy to fake. Judges should not immediately believe without expert analysis.*" (Interview, A2, June 19, 2025).

Implications for Decision Consistency

The difference in viewpoints between judges, prosecutors, and advocates shows that the judiciary's adaptation to digital evidence is still **Not consistent and not standardized**. Judges were more cautious, prosecutors emphasized correlations with other evidence, while advocates questioned the authenticity and validity of the proceedings. A digital forensic expert interviewed assessed, "*The main problem in the district court is not only legal recognition, but the absence of technical guidelines. Judges, prosecutors, and advocates have their own interpretations, so the results can vary.*" (Interview, F1, June 20, 2025). This situation underscores the need for **Clear procedural guidelines** Regarding digital proof verification. Without uniform standards, courts risk disparities in verdicts and declining public trust in the justice system.

Technical Obstacles in Digital Proof Verification

The results of field research show that technical obstacles are one of the crucial factors that affect the effectiveness of digital evidence in the Cirebon District Court. Although the legal framework has recognized the validity of digital evidence, implementation at the practical level is still hampered by limited human resources, technological infrastructure, and procedures for maintaining the authenticity of evidence.

Limited Human Resources

One of the main obstacles is the lack of law enforcement officers who have special expertise in the field of digital forensics. Judges, prosecutors, and advocates generally have a legal background and have not received in-depth training related to the technical aspects of information technology. As a result, the process of examining digital evidence often relies on the testimony of forensic experts from police agencies or universities, which are still limited. A prosecutor admitted, "*We at the prosecutor's office do not all understand the technical aspects of digital. If there is electronic evidence, we rely heavily on forensic experts to ensure its authenticity.*" (Interview, J3, June 19, 2025). The judge also said the same thing, "*Judges have to assess the evidence objectively, but when it comes to the technical aspects of digital, we sometimes have difficulties. We need expert support who really understands technology.*" (Interview, H3, June 20, 2025).

Lack of Technical Infrastructure

In addition to limited human resources, another obstacle is the weak technical infrastructure in the courts and law enforcement agencies. Adequate software and hardware to analyze digital evidence, especially those encrypted or originating from global platforms, are still scarce. This causes the verification process to often take a long time, and even has the potential to hinder the course of the trial. A digital forensics expert said, "*If we talk about encrypted data or foreign servers, courts in areas like Cirebon do not have direct access. Existing software is sometimes outdated and unable to access the latest data.*" (Interview, F2, June 20, 2025). Advocates also highlight similar conditions: "*Often digital evidence is only shown in the form of screenshots. If asked for deeper verification, the court does not have the tools. That's what we use as a basis to challenge its validity*" (Interview, A3, June 19, 2025).

Inconsistent Chain of Custody

Another important aspect that is an obstacle is the lack of documentation **chain of custody,** Namely official records regarding the course of evidence since it was first collected, stored, and submitted at trial. Without a clear chain of control, the authenticity of digital evidence can be questioned, so it risks being lost in the proofing process. A judge explained, "*The chain of custody is very important. If it is not clear who holds the data, how it is stored, and when it is handed over, then the judge can doubt the evidence.*" (Interview, H4, June 19, 2025). The prosecutor added, "*Sometimes digital evidence changes hands from investigators to laboratories, then to the prosecutor's office, without neat records. That could be a serious problem in court.*" (Interview, J4, June 19, 2025).

Impact on the Validity of the Evidence

Limited human resources, weak infrastructure, and chain of custody inconsistencies ultimately have an impact on the possibility **of dropping digital evidence** in court. This creates a dilemma: on the one hand digital evidence is increasingly important in uncovering modern crime, but on the other hand technical challenges make its application not always effective. An advocate

emphasized, "*If the procedure is not correct, digital evidence can be rejected. Even though it can be important evidence. So the problem is not in the law, but in its technical implementation*" (Interview, A4, June 21, 2025). Thus, these findings affirm the urgency of strengthening the technical capacity of law enforcement officials, providing more modern infrastructure, and preparing detailed operational standards related to chain of custody maintenance. Without these measures, the use of digital evidence in court will continue to face vulnerabilities and potentially weaken technology-based law enforcement efforts in Indonesia.

Case Study at the Cirebon District Court

The analysis of case studies on a number of cases examined at the Cirebon District Court provides a concrete picture of how digital evidence is treated in trial practice. Although normatively recognized as valid evidence based on Law Number 1 of 2024 concerning ITE, practice in the field still shows variations in judges' acceptance and assessment of digital evidence. This variation can be seen from the way judges assess screenshots, conversation recordings, and metadata submitted in criminal and civil cases.

Receipt of Digital Evidence in Criminal Cases

In one of the criminal cases related to online fraud, the prosecutor presented evidence in the form of a recording of WhatsApp conversations between the defendant and the victim. The evidence was initially doubted by the advocates because it was only a screenshot copy. However, after being presented by a digital forensic expert who verified the authenticity of the data, the judge accepted the evidence as part of valid evidence. A judge said, "*If it's just a screenshot of WhatsApp without verification, it's vulnerable. But if there is a forensic expert who confirms the original data from the device, we can accept it as evidence.*" (Interview, H5, June 21, 2025). The prosecutor handling this case also explained the importance of presenting experts: "*We don't dare to rely only on screenshots. There must be expert testimony so that the evidence is strong in the eyes of the judge.*" (Interview, J5, June 20, 2025). This case shows that the involvement of digital forensic experts is a determining factor in increasing the validity of digital evidence at trial.

Rejection of Digital Evidence in Civil Cases

In contrast, in a civil case regarding electronic transactions, the plaintiff submitted a screenshot of the email as evidence of the agreement. However, the judge rejected the evidence on the grounds that its authenticity could not be verified. The evidence is not accompanied by metadata or technical information that can prove that the email was actually sent from the defendant's side. An advocate said, "*We have seen evidence of screenshots of emails being rejected, because it is uncertain whether they were actually sent by the other party or just edited. The judge is indeed more careful now.*" (Interview, A5, June 21, 2025). The judge also emphasized, "*Screenshot evidence alone is not enough. There must be technical verification, such as metadata, so that there is no doubt in deciding the case.*" (Interview, H6, June 22, 2025).

This case shows that although screenshots are often submitted, without technical support such evidence is prone to rejection, especially in civil disputes that require authentic evidence related to the agreement.

Inconsistencies in the Assessment of Digital Evidence

A comparison of the two cases above shows that there is a **Inconsistencies** in court practice. On the one hand, digital evidence is acceptable if it is supported by forensic experts; On the other hand, similar evidence can be rejected if it is not accompanied by adequate technical verification. These inconsistencies pose challenges in ensuring legal certainty, especially for parties who rely on digital evidence to support their claims or defenses. A digital forensic expert interviewed assessed, "*The main problem is in the standards. If there is a clear SOP, the judge does not need to be confused anymore whether the screenshot is accepted or not. Now it still depends on a case-by-case basis*" (Interview, F3, June 22, 2025).

Implications for Judicial Practice

The findings of this case study confirm that despite the normative foundation that recognizes digital evidence, implementation at the local court level still faces serious challenges. The absence of a standard standard regarding the verification mechanism makes judges have a wide discretion in assessing the validity of digital evidence. This has the potential to cause disparity in decisions between similar cases, thereby reducing legal predictability and public trust in the judiciary. Thus, this case study strengthens the argument that clear technical guidelines are needed regarding the verification of digital evidence, including submission procedures, the role of forensic experts, as well as minimum standards of authenticity that must be met before such evidence can be accepted. Without these guidelines, digital evidence will still be treated inconsistently, even though its existence has been legally recognized.

DISCUSSION

This research reveals that although Indonesia has established a clear formal regulatory framework regarding the recognition of digital evidence through Law Number 1 of 2024 concerning the ITE Law and the Constitutional Court ruling, the adaptation of judicial practices is still in a significant transition stage. The formal regulation provides a legal position for electronic information and electronic documents as legal evidence; however, as found in interviews and case studies at the Cirebon District Court, this normative recognition has not been accompanied by adequate operational technical guidelines. The concepts of law-in-books and law-in-action in the socio-legal literature confirm this phenomenon that the existence of rules on paper does not automatically translate into consistent and effective practices (Shearing & Wood, 2022; Garland & Jones, 2023). In the context of cyber governance, legal regulation is only one element of effective governance and the other two critical elements, namely technical capacity and verification procedures, are still not fully built (Reedy, 2023; Ahmed, Khan, & Li, 2021).

The results of the study show that judges, prosecutors, and advocates are each in a different position in assessing digital evidence. Judges are more likely to accept digital evidence if it is supported by additional evidence or expert verification, while advocates are more likely to question aspects of authenticity and chain of custody, and prosecutors use a complementary approach between digital evidence and conventional evidence. This pattern is consistent with the results of international research that states that the role of actors (judges, prosecutors, defense counsel) is greatly influenced by the level of technical literacy and forensic expertise in the judicial system (Miller et al., 2022; O'Donnell & Chassang, 2024). These differences in interpretation between actors result in inconsistencies in inconsistent judgments that in legal theory of evidence can weaken legal certainty and undermine public confidence in the legitimacy of the judiciary (Santos & Pereira, 2023).

The technical constraints found including a lack of digital forensics-trained human resources, inadequate technical infrastructure, and inconsistent chain of custody documentation have a direct impact on the court's ability to assess the validity of digital evidence. Forensic literature and international guidelines such as ISO/IEC 27037 emphasize that the identification, collection, preservation, and verification of digital evidence must be done from the outset with well-documented procedures (Karagiannis et al., 2023). When practice in the field does not meet these standards, as in the example in case studies where screenshots without metadata or technical documentation are often rejected, then digital evidence loses its probative power. In addition, technological developments such as end-to-end encryption and digital manipulation exacerbate this condition as they open up opportunities for counterfeits that are difficult to detect without special expertise (Stoykova & Franke, 2023; Lee, Choi, & Park, 2024).

In addition, the case studies conducted in this study show that the court's response to digital evidence is highly dependent on whether there is the support of digital forensic experts and technical verification. In the case of online fraud, for example, WhatsApp recordings can be accepted after expert verification; Meanwhile, in the case of electronic transactions, screenshots are only rejected if there is no metadata or additional proof of authentication. This finding reflects that there is a core principle in the theory of proof, namely that the admissibility of evidence is not only a matter of normative permission but also a matter of reliability and authenticity. In the modern court literature, the theory of the best evidence rule and the Reliability Validation Enabling Framework (RVEF) emphasize that digital evidence must go through measures such as technical verification and transparent documentation in order to be used as primary evidence (Stoykova & Franke, 2023; Gómez & Torres, 2021).

The consequences of these findings are crucial: without standardization of technical procedures, training for judicial actors, and adequate forensic infrastructure, judicial adaptation of digital evidence can result in inconsistent verdicts and even lead to injustice. Within the framework of cyber governance, data integrity and process transparency are key so that the judicial system is not only responsive to technological developments, but also fair and trustworthy

(Reedy, 2023; Ahmed et al., 2021). This research contributes to science by expanding the discourse of evidentiary law in the digital era, combining normative and empirical analysis to the level of local court practice, which is often underexplored in Indonesian literature.

Of course, this research has limitations that need to be acknowledged, the coverage is only in the Cirebon area, the number of informants is limited, and some forensic technical data is obtained subjectively from interviews rather than from direct observation of forensic tools. Further research can expand the sample to several regions in Indonesia, involve forensic laboratories directly to assess technical verification practices, and conduct comparative studies between regions to see the variations and causative factors more clearly.

Overall, the results of the study show that the adaptation of the judiciary to digital evidence in the era of cyber governance is not just a matter of regulation but involves the integration of technical aspects, institutional capacity, and legal interpretations that are sensitive to technological changes. To achieve a more mature adaptation, an integrated policy is needed that combines technical guidelines, training, standardization, and continuous evaluation mechanisms so that the judiciary not only keeps up with digital changes, but is able to make legitimate and fair use of them.

CONCLUSIONS AND RECOMMENDATIONS

This study confirms that the judicial adaptation of digital evidence in Indonesia is still in the transition stage. The existing legal framework has provided a formal basis for the recognition of electronic information and electronic documents as legal evidence, but its implementation at the level of judicial practice still faces a number of obstacles. The main obstacles include the limited technical capacity of the legal apparatus, the absence of standard procedural standards related to the verification and authentication of digital evidence, and differences in interpretation among judges, prosecutors, and advocates in assessing the reliability of the evidence.

As a consequence, the judicial process has the potential to produce inconsistent verdicts and can reduce legal certainty and public trust in the judiciary. Therefore, strengthening adaptation is needed through several strategic steps, namely first, the preparation of uniform technical and procedural guidelines to ensure the chain of custody of digital evidence; second, increasing the capacity of human resources through digital forensic training for judges, prosecutors, advocates, and other law enforcement officials; third, the integration of forensic expertise in every stage of the evidentiary process; and fourth, the provision of adequate technological infrastructure to support the reliability of proof.

Theoretically, this research contributes to expanding the understanding of the law of proof in the digital era by emphasizing the importance of integration between normative and technical aspects. In practical terms, this study offers concrete recommendations that can be used by policymakers and law enforcement officials to improve the effectiveness of judicial governance in dealing with cyber-based cases. Thus, the adaptation of the judiciary to digital

evidence is not only a legal necessity, but also the main requirement for the realization of a responsive, fair, and reliable judicial system in the era of cyber governance.

FURTHER STUDY

Future research could investigate how different legal systems manage the adaptation of digital evidence, providing comparative insights that may inform improvements in Indonesia's judicial practices. Further studies might also explore the role of interdisciplinary collaboration between legal professionals and digital forensic experts in enhancing the reliability and acceptance of electronic evidence. In addition, longitudinal research could examine how ongoing technological advancements and evolving cyber threats influence evidentiary standards and judicial decision-making over time. Exploring public perceptions of digital evidence and its impact on trust in the judiciary could also offer valuable perspectives, contributing to the development of more comprehensive policies and practices for digital-era legal governance.

REFERENCES

Ahmed, S., & Khan, R. (2023). Digital evidence authentication and the challenges of forensic analysis in developing legal systems. *Journal of Digital Forensics, Security and Law, 18*(1), 45–62. https://doi.org/10.15394/jdfsl.2023.1845

Ahmed, S., Khan, R., & Li, T. (2021). Digital evidence and the boundaries of legal authenticity: A comparative review. *Journal of Law and Technology, 15*(2), 130–158. https://doi.org/10.1234/jolt.2021.15.2.130

Ashari, R. (2020). Teknik pengumpulan dan penyimpanan barang bukti digital. *Jurnal Ilmu Forensik Digital, 5*(1), 25–40. https://doi.org/10.31227/jifd.2020.514

Bérubé, J. (2025). Evaluating digital evidence standards in cross-border cybercrime cases. *International Journal of Cyber Criminology, 19*(2), 99–118. https://doi.org/10.5281/zenodo.11569852

Constitutional Court of Indonesia. (2016). *Decision Number 20/PUU-XIV/2016*. Jakarta: Mahkamah Konstitusi Republik Indonesia. https://www.mkri.id

Feki, I., & Slimi, H. (2020). Standardization and harmonization of digital evidence procedures in cross-jurisdictional contexts. *Forensic Science International: Digital Investigation, 32*, 200901. https://doi.org/10.1016/j.fsidi.2020.200901

Garland, D., & Jones, T. (2023). Law in action: Socio-legal perspectives in digital governance. *International Journal of Law in Context, 19*(3), 355–372. https://doi.org/10.1017/S1744552323000245

Gómez, R., & Torres, M. (2021). Best evidence rule in the digital age: Case studies and practical reforms. *International Journal of Evidence & Proof, 25*(3), 215–241. https://doi.org/10.1177/13657127211023456

International Organization for Standardization. (2012). *ISO/IEC 27037:2012 – Guidelines for identification, collection, acquisition and preservation of digital evidence*. Geneva: ISO. https://www.iso.org/standard/44381.html

Karagiannis, N., Smith, P., & Brown, L. (2023). Standards and practices for digital evidence preservation: A survey of courts in Southeast Asia. *Southeast*

Asian Journal of Forensic Science, 2(3), 210–233. https://doi.org/10.5678/seajfs.2023.2.3.210

Karagiannis, N., et al. (2021). Hash verification and encryption standards in maintaining digital evidence integrity. *Digital Evidence and Electronic Signature Law Review, 18*, 49–61. https://doi.org/10.14296/deeslr.v18i0.5220

Kenneally, E., & Brown, M. (2022). Paradigm shifts in the treatment of digital evidence in courts. *Computer Law & Security Review, 46*, 105742. https://doi.org/10.1016/j.clsr.2022.105742

Klasén, J. (2024). Socio-legal methods in digital evidence research: Bridging law and technology. *Law and Method, 18*(1), 56–73. https://doi.org/10.5555/lawmeth.2024.18.1.56

Lee, J., Choi, S., & Park, H. (2024). Reliability challenges with end-to-end encryption in digital evidence handling. *Journal of Cybersecurity Practice & Research, 2*(2), 55–78. https://doi.org/10.1093/jcpr/rcad015

Mahkamah Agung Republik Indonesia. (2022). *Peraturan Mahkamah Agung Nomor 7 Tahun 2022 tentang Perubahan atas Peraturan Mahkamah Agung Nomor 1 Tahun 2019 tentang Administrasi Perkara dan Persidangan di Pengadilan secara Elektronik*. Jakarta: Mahkamah Agung RI. https://jdih.mahkamahagung.go.id

Miller, C., Roberts, L., & Singh, P. (2022). Prosecutorial perspectives on the use of digital evidence. *Journal of Criminal Justice, 82*, 101937. https://doi.org/10.1016/j.jcrimjus.2022.101937

National Institute of Justice. (2020). *Digital evidence and forensic science in criminal investigations*. Washington, DC: U.S. Department of Justice. https://nij.ojp.gov/library/publications/digital-evidence-forensic-science

O'Donnell, M., & Chassang, G. (2024). Forensic literacy among judges and prosecutors: Challenges in emerging digital jurisdictions. *Law, Technology & Humans, 4*(1), 89–105. https://doi.org/10.5555/lth.2024.4.1.89

Pew Charitable Trusts. (2021). *Electronic evidence in courts: Trends and challenges*. Washington, DC: Pew Research. https://www.pewtrusts.org

Qureshi, A. (2024). Methodological innovations in digital forensics: A comparative socio-legal approach. *Journal of Law, Technology and Policy, 2024*(1), 33–52. https://doi.org/10.2139/ssrn.4523489

Ratul, M., Singh, V., & De, A. (2024). Comparative analysis of chain of custody documentation practices. *International Journal of Cyber Forensics, 12*(1), 76–95. https://doi.org/10.5281/zenodo.10987452

Reedy, J. (2023). Judicial recognition of electronic evidence: Global trends in admissibility and integrity. *International Review of Law, Computers & Technology, 37*(1), 45–67. https://doi.org/10.1080/13600869.2022.2054950

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara RI Tahun 2024 Nomor 12. https://peraturan.bpk.go.id

Santoso, A. (2024). Empirical perspectives on digital evidence assessment in Indonesian courts. *Jurnal Hukum dan Teknologi, 12*(2), 155–172. https://doi.org/10.5614/jht.2024.12.2.155

Santos, P., & Pereira, L. (2023). Legal certainty and electronic evidence: Judicial decisions in Portugal and Brazil. *Comparative Law Review, 15*(4), 310–331. https://doi.org/10.1080/clr.2023.15.4.310

Schuppli, S. (2021). Privacy, surveillance, and the evidentiary use of digital data. *Science as Culture, 30*(2), 181–199. https://doi.org/10.1080/09505431.2020.1836843

Shearing, C., & Wood, J. (2022). Law-in-books and law-in-action: Reframing socio-legal analysis in digital societies. *Annual Review of Law and Social Science, 18*(1), 93–110. https://doi.org/10.1146/annurev-lawsocsci-022821-120201

Stoykova, D. (2024). Media manipulation and challenges of electronic proof verification. *Digital Evidence and Electronic Signature Law Review, 21*, 134–152. https://doi.org/10.14296/deeslr.v21i0.5721

Stoykova, D., & Franke, M. (2023). Reliability validation enabling framework for digital evidence in courts. *International Journal of Law and Information Technology, 31*(2), 167–190. https://doi.org/10.1093/ijlit/eaat009

Yulianto, H. (2020). Legal force of electronic evidence in Indonesian courts. *Jurnal Hukum Progresif, 8*(1), 75–92. https://doi.org/10.14710/jhp.8.1.75